Chapter 12

From the Secret of Apollo to the Lessons of Failure

The Uses and Abuses of Systems Engineering and Project Management at NASA

Stephen B. Johnson

In his books, *To Engineer Is Human*[1] and *Success through Failure*,[2] Henry Petroski has documented an interesting and important relationship between an engineering discipline and the reliability of the technical products that it produces. He found that over the course of several generations of engineers in a given discipline, such as civil engineers specializing in bridge building, that the reliability (or conversely, the failure rate) of their products swings back and forth from highly conservative, highly reliable designs to more innovative, less reliable designs. Ultimately the less reliable designs lead to outright failure, such as the famous Tacoma Narrows Bridge failure of 1940. This prompts engineers to determine the causes of the failure and implement more conservative designs on their next projects. Eventually, after many successes, some designers reduce "excessive" design margins to save money, to improve performance, or simply to try new ideas. Eventually someone goes too far and creates a design with inadequate margins, leading once again to failure. Petroski's examples came from civil engineering, but he found this same pattern in other engineering disciplines, including aerospace. He noted that the tragic losses of the Space Shuttles *Challenger* in 1986 and *Columbia* in 2003 follow the same pattern.[3]

---

1. Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (New York, NY: St. Martin's Press, 1982).
2. Henry Petroski, *Success through Failure: The Paradox of Design* (Princeton, NJ: Princeton University Press, 2006).
3. Ibid., pp. 163–167.

Petroski's analysis is relevant to NASA because he emphasizes multigenerational knowledge transfer and learning in engineering design and how changes in the perception of risk affect failure rates. NASA has a strong tradition of research and system development, and it also operated these systems, creating organizations focused on launch and mission operations. Understanding NASA's ability to create and operate complex systems requires an understanding of both its large-scale engineering development and its operation of these systems. While academic researchers of "high reliability organizations" have studied operations of complex, high-risk systems such as aircraft carriers and nuclear power plants, there is a relative dearth of research on the dependability of engineering design.[4] Such research is needed, given the emerging understanding that one of NASA's fundamental issues is its culture.

In the 1960s, NASA's Apollo program was a shining example of what humans could accomplish when they set their minds to achieving a difficult goal. As many noted at the time, it was an incredible feat of organization as well as technology. NASA's ability to direct hundreds of thousands of factory workers, engineers, scientists, and managers to achieve multiple lunar landings drew accolades in the United States and abroad.

Yet 31 years after the last astronaut left the lunar surface, the loss of NASA's second Space Shuttle, *Columbia*, and its seven astronauts left the Agency devastated and distraught. The *Challenger* disaster in January 1986 was a shock, shattering NASA's aura of invincibility. The loss of *Columbia* in February 2003 implied more fundamental problems. No longer could the blame for an accident be placed on a few overconfident engineers or managers. Something inherent to NASA as an institution was flawed, something the Columbia Accident Investigation Board identified as NASA's "culture."

"Culture" is a famously holistic and ambiguous term, even for social scientists who use it in their daily work. According to *Webster's Ninth New Collegiate Dictionary*, culture is "an integrated pattern of human knowledge, belief, and behavior that depends upon man's capacity for learning and transmitting knowledge to succeeding generations," or "the customary beliefs, social forms,

---

4. See, for example, T. R. LaPorte, "High Reliability Organizations: Unlikely, Demanding, and at Risk," *Journal of Crisis and Contingency Management* 4, no. 2 (June 1996): 55–59; K. H. Roberts, "New Challenges to Organizational Research: High Reliability Organizations," *Industrial Crisis Quarterly* 3 (1989): 111–125; and K. E. Weick, "Organizational Culture as a source of high reliability," *California Management Review* 29 (1987): 112–127. Much of this research is a response to Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York, NY: Basic Books, 1984), which argued that accidents are almost inevitable or "normal" in complex systems.

and material traits of a racial, religious, or social group."[5] While accurate, this diagnosis was problematic for NASA. Which beliefs, social forms, or material traits did NASA need to change? The Columbia Accident Investigation Board did not elaborate.

From a historical perspective, was the NASA culture that produced the amazing feats of the 1960s the same culture that also created the disasters of 1986 and 2003? If not, then what changed? Furthermore, can we pinpoint the specific beliefs, social forms, or material traits within NASA's people and organization that cause failure? As NASA celebrates its 50th anniversary in 2008 and embarks on a new journey back to the Moon, can it recreate the magic of Apollo, or will its cultural baggage set the stage for a tragedy in deep space? The fate of America's civilian space agency, and perhaps of humanity's future in space, depends critically on whether NASA understands and can improve its culture sufficiently to make long-term endeavors in deep space viable.

NASA's Original Technical Culture

Between October 1958, when NASA began operations, and July 1960, NASA acquired a number of research and development organizations. From the NACA, NASA inherited three research Centers: Langley, Lewis, and Ames. From NRL, NASA acquired the Vanguard division, which formed the base of GSFC. The Army transferred Caltech's JPL to NASA control as well as the ABMA, which became MSFC. NASA also acquired some projects from the U.S. Air Force, including the F-1 engine used for the Saturn launch vehicle. NASA Headquarters attempted to weld these disparate organizations into a coherent agency.[6]

Despite their differences, these organizations shared some common characteristics, which political scientist Howard McCurdy has identified as NASA's "original technical culture." A strong "in-house" technical competence was shared among all of NASA's original organizations and personnel. They had decades of experience of hands-on technical work and were at least as competent as the contractors that NASA managed as it grew in the 1960s. A crucial part of NASA's technical competence was its insistence on rigorous testing, which grew more elaborate along with NASA's machines. NASA also prided itself on its exceptional personnel. Its original staff members and those it hired in the expansion years of the early 1960s were among the best and brightest that

5. *Webster's Ninth New Collegiate Dictionary* (Springfield, MA: Merriam-Webster, Inc., 1991).
6. Howard E. McCurdy, *Inside NASA: High Technology and Organizational Change in the U.S. Space Program* (Baltimore, MD: Johns Hopkins University Press, 1993), chap. 1.

the United States (and its allies!) had to offer. Spaceflight had a glamour and excitement in the 1960s that attracted exceptionally bright and talented staff.[7]

A key organization for Apollo, and unique in its heritage and capabilities, was MSFC's "Rocket Team" under Wernher von Braun. Von Braun himself was one of the founders of rocket technology, as the leader of the V-2 project in Nazi Germany. He was by all accounts a charismatic visionary, an extraordinary manager, a technical leader, and a cultured, charming man. His team of German engineers had been together for decades, working on the same technology throughout that time. They all knew their tasks and how they related to the tasks of their team members. Von Braun, in 1963, described his management style as that of a gardener nurturing and cultivating a capability grown over years, a rather accurate description of the evolution of his team.[8]

Von Braun used simple but effective methods that capitalized on this experienced, "organic" group. He used a policy of "automatic responsibility," whereby division leaders, and even low-level engineers, were required to take responsibility to resolve problems they uncovered, even outside of their own local organizations. If the problem was outside of their area, they were required to alert the relevant organizations of the issue, at which point they were then "automatically responsible" to resolve them. For difficult technical issues, he chaired meetings where the key parties openly debated their views and disagreements. Von Braun would summarize and explain the issues, and then he would make a decision as to how the organization would proceed. By the late 1960s, von Braun also implemented a system of "Monday Notes," whereby all of the division leads would submit a single page of their major issues to von Braun, who would then comment on the full set of notes and circulate them to the entire team. These relatively informal but rigorous techniques worked well due to von Braun's tact and competence and the intimate knowledge that each team member had with other team members.[9]

With the exception of MSFC's unique group, by and large, NASA's extremely experienced and competent engineers and scientists were not particularly

---

7. McCurdy, *Inside NASA*, chap. 2.
8. Michael J. Neufeld, *Von Braun: Dreamer of Space, Engineer of War* (New York, NY: Vintage Books, 2007); Wernher von Braun, "Management of Manned Space Programs," in *Science, Technology, and Management*, ed. Fremont E. Kast and James E. Rosenzweig (New York, NY: McGraw-Hill, 1963).
9. Phillip K. Tompkins, *Organizational Communication Imperatives: Lessons of the Space Program* (Los Angeles, CA: Roxbury, 1993), pp. 62–70; Yasushi Sato, "Local Engineering and Systems Engineering: Cultural Conflict at NASA's Marshall Space Flight Center, 1960–1966," *Technology and Culture* 46, no. 3 (July 2005): 570–575.

good at managing large, complex projects. The NACA's engineers trained on high-technology programs, but these were typically in association with contractors and often with DOD, which managed the truly large-scale programs and manufacturing capabilities. Engineers and scientists from JPL and NRL had similar backgrounds, and they were frequently researchers more than designers or project managers. NASA primarily organized itself by informal committees, ultimately reaching the point where, on the Mercury project, it created a committee to organize the other committees.[10] To remedy this chaotic situation, NASA hired George Mueller in 1963 from TRW's Space Technology Laboratories to head the Office of Manned Space Flight. Mueller quickly realized that he needed to reorganize NASA Headquarters to convert its hands-on engineers into executive managers and that he needed help from outside of NASA to manage the massive Apollo program.[11]

Mueller's most important recruit was Minuteman ICBM Program Manager Samuel Phillips. Phillips had made a name for himself as a manager by bringing this large and complex project to deployment on time and under budget, a rarity for large aerospace projects. The Air Force agreed to assign Phillips to NASA, but only if he became Apollo Program Manager. In January 1964, Phillips submitted a request to his former boss, Air Force Systems Command Chief Bernard Schriever, for further Air Force personnel to be assigned to Apollo to help manage the massive program. Schriever agreed and transferred over 150 senior, middle, and junior officers to NASA.[12]

Mueller, Phillips, and their military cohorts brought to NASA a management system developed during the previous 15 years of ballistic missile development. This included several key elements; the most prominent were concurrency, change control and configuration management, environmental testing, systems engineering, phased planning, and project management.

- *Concurrency* was a method to speed up development by designing, developing, manufacturing, and testing a missile's various pieces and support systems in parallel. This required more detailed planning than serial design and development, since changes in one component often impacted related components, causing simultaneous changes.

---

10. Stephen B. Johnson, *The Secret of Apollo: Systems Management in American and European Space Programs* (Baltimore, MD: Johns Hopkins University Press, 2002), pp. 116–120.
11. W. Henry Lambright, *Powering Apollo: James E. Webb of NASA* (Baltimore, MD: Johns Hopkins University Press, 1995): 114–118; Johnson, *The Secret of Apollo*, pp. 130–135.
12. Johnson, *Secret of Apollo*, pp. 135–137.

- To handle this problem, engineers developed *change control* so that changes in one component had to be approved by a central systems engineer who coordinated the impacts of those changes on other components.
- *Configuration management* was the use of change control by managers to ensure that cost and schedule estimates were submitted along with each technical change, so as to predict its cost and schedule ramifications. This gained managers some cost and schedule prediction capability through the ability to veto changes that were too expensive or delayed schedules.
- *Environmental testing* improved system reliability by testing a prototype design in a simulated environment in which system components had to operate, such as the projected temperature ranges, vibration levels, and vacuum environment.
- *Phased planning* provided top-level managers with checkpoints in the project's development cycle, at which managers could cancel a project if it was projected to have insurmountable technical, cost, or schedule risks.
- *Systems engineering* encompassed all of these facets, including systems analysis to trade off potential design solutions.
- *Project management* organized a project on the basis of its technical products, as opposed to the disciplines from which the individuals that staffed the project were drawn. Each portion of a project organization was organized around its individual product, such as a structure, a guidance system, or a rocket engine.

These techniques evolved as responses to technical or managerial failings within the Air Force during the 1950s. For example, project management was implemented in response to management issues in early 1950s missile projects, where personnel being yanked from one group to another by line management in charge of many projects left critical projects without needed staff. Change control and environmental testing were responses to ballistic missile test failures caused by mismatched components when design changes had not been communicated between different groups, or components failed due to unexpected environmental factors. Configuration management and phased planning were responses to cost and schedule overruns on a variety of large scale military development programs.[13]

---

13. Ibid., chaps. 2 and 3; Thomas P. Hughes, *Rescuing Prometheus* (New York, NY: Pantheon, 1998), pp. 106–139.

Recognizing Apollo's size and complexity, NASA brought top-level management of the entire program to NASA Headquarters. At Administrator James Webb's insistence, Headquarters hired General Electric and Bellcomm (an offshoot of American Telephone and Telegraph specifically established for the purpose) to provide Apollo program support to Headquarters.[14] By the late 1960s, Headquarters was controlling cost and schedules through Phillips's system of configuration management. To make it work, Phillips needed NASA's unruly designers to define Apollo's actual design. Once defined, this "technical baseline" could be "frozen." This baseline configuration would not be changed unless a change request was made with proper technical, cost, and schedule justification. While Phillips faced a number of objections from MSFC and JSC management who were not eager to be controlled by Phillips's system, through persistence and persuasion by the end of 1966, he was well on his way to full implementation of this system, collectively called "systems management," over Apollo's technical committees.[15]

Failures of the 1960s: Strengthening Systems Management

In the early planetary programs of the late 1950s and early 1960s, a similar evolution from simple committee structures and processes to more sophisticated and bureaucratic methods occurred. The Jet Propulsion Laboratory began in World War II as an Army-funded organization to develop ballistic missiles. During the development of the Corporal missile, JPL ran into the same difficulties with missile failures and cost and schedule overruns as the Air Force had in its ballistic missile programs, and it developed the same kinds of solutions. It implemented these solutions, enumerated in the previous section, in the follow-on Sergeant program, resulting in much higher reliability in Sergeant than Corporal.[16]

After the launch of Sputnik in October 1957 and the subsequent failure of Vanguard's first launch attempt two months later, JPL Director William Pickering gained Army approval to build the satellite for the Army's first attempt to place a spacecraft in orbit, Explorer 1. Its success in January 1958 and JPL's subsequent transfer to NASA the next year put JPL on the path to lead NASA's planetary exploration. In the race against the Soviet Union into space, JPL placed a higher priority on speed than on reliability, and not surprisingly, its

14. Johnson, *Secret of Apollo*, pp. 124–125.
15. Ibid., pp. 139–141; Stephen B. Johnson, "Samuel Phillips and the Taming of Apollo," *Technology and Culture* 42, no. 4 (October 2001): 683–709.
16. Johnson, *Secret of Apollo*, pp. 80–99.

early satellites had a high rate of failure, roughly 50 percent in the late 1950s and early 1960s. However, on the Ranger program, which was to take close-up pictures of the lunar surface just prior to crashing into it, a series of six consecutive failures proved more than was politically acceptable. These failures led to congressional investigations of the implementation on Ranger and all of JPL's later spacecraft of the methods evolved from Corporal and deployed on Sergeant. Having already deployed and improved these methods on the Mariner project to send a spacecraft to Venus in 1962, Mariner Project Manager Jack James spearheaded JPL's early efforts to deploy them on other JPL projects and NASA robotic spacecraft programs. These systems engineering methods dramatically improved the reliability of JPL's spacecraft from then on.[17]

In the meantime, Apollo continued rapidly forward in its determination to land an American astronaut on the Moon before the Soviets. By 1966, Samuel Phillips's implementation of systems management techniques was well under way but hardly complete. When three astronauts died on the launchpad on 27 January 1967 during a prelaunch test, the resulting investigation put Apollo and its management methods under the microscope. The accident investigation, run by NASA, concluded that the Agency had severely underestimated the danger of a pure oxygen atmosphere at sea level pressure. The Apollo 204 fire had been caused by a spark in the Apollo Command Module, which ignited the pressurized, pure oxygen atmosphere. Earlier warnings about the potential danger from General Electric safety personnel had been forwarded to NASA, whose safety groups concluded that the risk was acceptable.[18]

Phillips's methods survived the scrutiny unscathed and even strengthened. He had been actively implementing configuration management over NASA's committee structures since his arrival at NASA, and he had uncovered problems with North American Aviation, the prime contractor for the Apollo Command Module and Saturn second stage. By its silence about Phillips's methods, the investigative team and Congress sanctioned Phillips's techniques. In an interesting brief sentence, Congress noted cultural issues played a role: "The committee can only conclude that NASA's long history of testing and launching space vehicles with pure oxygen environments at 15.7 psi and lower pressures led

17. Ibid., pp. 92–114.
18. Johnson, *Secret of Apollo*, pp. 145–147; Mike Gray, *Angle of Attack: Harrison Storms and the Race to the Moon* (New York, NY: Penguin, 1992), pp. 232–235; Alexander Brown, "Accidents, Engineering, and History at NASA, 1967–2003," in *Critical Issues in the History of Spaceflight*, ed. Steven J. Dick and Roger D. Launius (Washington, DC: NASA SP-2006-4702, 2006), pp. 379–383.

to overconfidence and complacency." Success bred complacency and created the conditions for future failure.[19]

In the fire's aftermath, NASA made many technical design improvements to Apollo and implemented a new safety system, while Phillips implemented more project reviews and strengthened configuration control.[20] Apollo went on to a series of spectacular successes. These included the first piloted lunar landing of Apollo 11, the near-disaster and heroic recovery of Apollo 13, and several valuable science missions up to Apollo 17. After the successful Apollo 11 landing in July 1969, a congressional hearing and staff study gave NASA the opportunity to showcase its management system, which was widely believed to be one of the primary reasons for Apollo's success. With Apollo, NASA had earned a reputation as an organization capable of incredible technical feats. NASA was an extraordinarily competent and confident institution. However, NASA's competence would soon begin to erode, and its confidence would be ultimately misplaced.[21]

Weakening Systems Management: To *Challenger*, Hubble, and Mars Observer

From its inception in 1958 through the early 1960s, NASA's workforce grew dramatically, up to 36,000 in 1967, and the contractor force working for NASA grew even faster, peaking at roughly 300,000 in 1966. After that time, NASA's workforce slowly declined, and the contractor workforce dramatically shrank, down to 100,000 by 1972. NASA was generally able to reduce its force through regular attrition, though from 1972 to 1975, NASA had to lay off workers. NASA's workforce decline was over by the early 1980s, with roughly 22,000 personnel in 1982. From 1967 through the 1980s, NASA's hiring remained anemic, and the average age of NASA's technical personnel peaked in 1982 at 44.5 years old.[22]

---

19. Johnson, *Secret of Apollo*, pp. 143–150; Nancy G. Leveson, "Technical and Managerial Factors in the NASA Challenger and Columbia Losses: Looking Forward to the Future," in *Controversies in Science & Technology: From Climate to Chromosomes*, ed. Daniel Lee Kleinman, Karen A. Cloud-Hansen, Christina Matta, and Jo Handelsman (New Rochelle, NY: Mary Ann Liebert, 2008), p. 257. Quotation from Senate Committee on Astronautical and Space Sciences, *Apollo 204 Accident*, 90th Cong., 2nd sess., 30 January 1968, with additional views, pp. 9–10.
20. Johnson, *Secret of Apollo*, pp. 143–150. Phillips's centralization went too far by 1968, slowing the program's progress, and Phillips relaxed some of his new overzealous rules that brought the smallest modifications to the attention of executive management.
21. House Committee on Science and Astronautics, *Apollo Program Management*, Staff Study for the Subcommittee on NASA Oversight, 91st Cong., 1st sess., July 1969.
22. McCurdy, *Inside NASA*, pp. 101–106.

In the meantime, in January 1972, President Richard Nixon approved NASA's next major human spaceflight program, the Space Shuttle. The Shuttle Program was sold on the basis that it would provide low-cost access to space. NASA intended it to become the sole transport system for all U.S. payloads and astronauts. To enable this, NASA needed the support of the Air Force. The Air Force needed the Shuttle to have a much larger payload bay able to deploy reconnaissance satellites, and a larger cross-range capability, which required larger wings to maneuver in the atmosphere. However, funding was limited in the 1970s, and Nixon approved a $5.5 billion development program, which was far less than what NASA needed to develop a fully reusable system. This limitation forced design changes on the Shuttle Program, making the Shuttle only partly reusable, using a throwaway external tank and SRBs that could be refurbished between flights. In combination, these conflicting goals and insufficient development funds put strains on the Shuttle Program that would contribute to its later failures.[23]

The Shuttle's development proceeded during the 1970s, and it was organized with the "lead Center" concept, whereby JSC led the program, instead of NASA Headquarters as on Apollo. Because JSC was at the same institutional level as MSFC and KSC, it had less clout for the Shuttle than NASA Headquarters had had for Apollo. Despite a number of technical problems, including the complicated SSME and the novel tiles of the orbiter's thermal protection system, the Shuttle's development proceeded, though with some delays and cost increases. The first flight of the Space Shuttle in April 1981 was perhaps the riskiest mission NASA ever attempted. This was the first, and to date the only, time a new launch vehicle's first test flight had astronauts on board. While successful, it showed NASA's extreme self-confidence at the time. Despite the loss of over one-third of its civil servants and two-thirds of its contract personnel, those that remained were very experienced and were able to pull it off. This further confirmed NASA's confidence in its own abilities.[24]

However, subtle shifts in NASA's engineering and management practices, as well as changes in the attitudes of its personnel, were weakening the Agency's abilities. NASA's goals remained ambitious, yet the sudden drop in funding in the early 1970s and its continued tightness through the early 1980s made

23. T. A. Heppenheimer, *The Space Shuttle Decision: NASA's Search for a Reusable Space Vehicle* (Washington, DC: NASA SP-4221, 1999), chap. 9.
24. T. A. Heppenheimer, *Development of the Space Shuttle 1972–1981: History of the Space Shuttle*, vol. 2 (Washington, DC: Smithsonian Institution Press, 2002).

the achievement of these ambitions problematic. At the same time, the federal government levied more regulations on the Agency to ensure external oversight and compliance with other goals such as workplace and environmental safety and workforce diversity. These new regulations drove an ever-larger burden of paperwork and a corresponding increase in administrative personnel as compared to technical workers. This made NASA a less desirable place to work as compared to its glory days in the 1960s; NASA had more paperwork and less hands-on engineering. The increasing regulations decreased the Agency's decision-making flexibility, with more weight given to cost and schedule factors, along with other regulations. Promotions were harder to come by, and with fewer jobs available, many highly qualified personnel took less demanding positions simply to remain employed. With fewer projects, and those few projects now under greater levels of scrutiny, the management of these projects became more averse to risk, while being required to pay closer attention to schedules and budgets. As a result of all these factors, morale suffered.[25]

Within the Shuttle Program, these factors combined to create conditions that made catastrophic decisions almost inevitable. In particular, MSFC, which was the institution in charge of the SSMEs, SRBs, and the external tank, underwent a number of changes after Apollo that weakened its abilities. The first was the loss of von Braun himself, who left MSFC in 1970. Von Braun's deputy, Eberhard Rees, was MSFC Director until 1973. Rocco Petrone took over until 1974, followed by William Lucas, who was Director from 1974 until the aftermath of the *Challenger* accident in 1986. While Rees understood von Braun's management system, neither Petrone nor Lucas caught its nuances. As the German team retired or were forced out (as many of them believed occurred under Petrone's regime), the informal bonds of von Braun's "organic" team broke down, while a formal system of systems engineering had not really taken hold at MSFC.[26]

Up to and through the 1960s, von Braun's team neither needed nor wanted systems engineering, which is in essence a formal method to ensure proper communications among different engineers and their disciplines in building a product. The German team did not need formal coordination methods, as they knew what to do and when to do it. Von Braun insulated systems engineering and Phillips's centralizing methods from MSFC's core engineering laboratories

25. McCurdy, *Inside NASA*, pp. 90–124.
26. Andrew J. Dunar and Stephen P. Waring, *Power to Explore: A History of Marshall Space Flight Center 1960–1990* (Washington, DC: NASA SP-4313, 1999), pp. 152–169.

and committees by placing systems engineering in the Industrial Operations Directorate (IOD), created in 1962. The Directorate was ultimately headed by Air Force Colonel Edmund O'Connor, whom Samuel Phillips recommended to von Braun to lead the new organization in September 1964. The relationship between Phillips and O'Connor ensured close communication between Headquarters and MSFC, while IOD minimized the impact of Phillips's Air Force-based processes on MSFC's less formal methods, which were the standard techniques in R&D Operations, where the various MSFC laboratories were institutionally housed. Though MSFC began to adopt systems engineering in the 1960s, not all parts of the organization fully accepted it.[27]

Finally, personalities mattered. William Lucas, MSFC's Director from 1974 to 1986, was an extremely intelligent, but difficult, person to work with. Lucas demanded precision from his MSFC managers and engineers, but, unlike von Braun, he did not appreciate hearing of bad news. Whereas von Braun sought out problems and rewarded those that brought problems into the open, Lucas often grew angry when he learned of problems, with a "shoot the messenger" attitude. Engineers at MSFC worked very hard to avoid mistakes, so as not to face Lucas's wrath. However, this also inhibited open discussions, since few were willing to talk about their work until they had done everything possible to prepare for a technical grilling. Lucas also modified the "Monday Notes" system, which became a method of upward communication only, without von Braun's commentary and feedback. Lucas used systems engineering reviews and configuration management to control MSFC's portions of the Shuttle Program, but the underlying attitude of fear and the resulting lack of communication subverted one of the primary goals of systems engineering, which is to enhance communication and ensure proper cross-checks and balances in the engineering design and decision process.[28]

While none of these issues alone caused the *Challenger* accident of 28 January 1986, they all contributed to the continuation of problems with the Shuttle's SRBs and to the fatal decision to launch the Shuttle despite record cold temperatures and a recommendation from the contractor, Thiokol, that the flight should be delayed. Problems with the SRBs had manifested themselves

---

27. Johnson, *Secret of Apollo*, pp. 150–152; Sato, "Local Engineering and Systems Engineering," pp. 564–578; Tompkins, *Organizational Communication Imperatives*, pp. 76, 88–90. Even as late as the early 1990s, some pockets of resistance to systems engineering remained, as propulsion experts claimed that systems engineering is "what all good engineers do." Author's recollection of meetings at MSFC from that time period.
28. Tompkins, *Organizational Communication Imperatives*, chap. 10.

starting in November 1981 with the flight of Space Transportation System (STS)-2, when the first incident of O-ring erosion (partial burning and charring of the rings) was detected after the flight. Efforts to understand and fix the problem found a number of issues, including problems with the putty that insulated the rings from the SRB flames in flight, rotation of the joint, and some stiffness in the rings in lower temperatures. Further O-ring erosion incidents occurred, but from that time until 1986, engineers and managers ultimately decided that the Shuttle could continue to fly, sometimes citing the fact that the system had a redundant O-ring. Even though tests had shown by 1978 that the second O-ring was ineffective as a backup, not until 1982 was the SRB joint design considered nonredundant, and even after that time, decision-makers continued to treat the design as if its redundancy was effective. Over time, O-ring erosion became classified as typical and acceptable behavior.[29]

On the night of 27 January 1986, with record cold predicted for the next day's launch, a Flight Readiness Review (FRR) teleconference was held to decide whether the Shuttle would fly the next morning. For the first time ever, Thiokol engineers, concerned that the low temperature would stiffen the O-rings sufficiently to cause them to fail in flight (allowing the hot gases to blow through the rings), recommended that the launch be delayed. Inquiring further to understand the recommendation's basis, NASA engineers and managers aggressively questioned Thiokol and concluded that Thiokol's argument, constructed quickly earlier in the day, was technically flawed. This was based largely on the existence of various kinds of problems associated with the SRBs described above and the inability of Thiokol engineers to differentiate temperature effects from other causes. Caucusing privately with the phone on "mute," Thiokol managers and engineers agreed with NASA's point that they could not prove that the SRBs would fail. Thiokol managers decided to reverse their recommendation, and the flight went forward the next morning.[30]

During the course of the discussions that evening, the essential point of an FRR had been unconsciously subverted. The FRR was intended to prove that the Shuttle could fly. Sufficient doubt about this should have been sufficient

---

29. Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago, IL: University of Chicago Press, 1996), chap. 4; Leveson, "Technical and Managerial Factors," pp. 247–251. Vaughan claims that NASA treated O-ring erosion as "normal," while Leveson disagrees, stating that NASA considered it "acceptable," though not normal. I treat this issue in the last section, essentially claiming that this behavior was no longer considered "anomalous" by some members of the community.
30. Vaughan, *Challenger Launch Decision*, chap. 8.

to stop the launch. Unfortunately, NASA's intense questioning raised doubts at Thiokol about their own arguments and gave the impression that NASA disagreed with them. Given that NASA ultimately had technical and funding authority over Thiokol, the contractor decided it could not press the point against its customer when it could not prove its case. Other NASA personnel who had doubts did not speak up. Thiokol should not have had to prove the case, and NASA management fatally accepted the changed position.[31]

In the aftermath of the *Challenger* accident, the Rogers Commission concluded that NASA's decision-making processes had been fundamentally flawed, largely due to communication problems between engineering and management personnel and their differing perspectives. The commission noted that the safety program on the Shuttle was significantly weakened in comparison to Apollo, and it was effectively "silent" regarding the problems leading to *Challenger*. This was due in part to safety functions being part of the program, with little independence from the Program Manager, who had to account for cost and schedule concerns. The commission included indictments of faulty information flows and the fact that executive management did not receive information about O-ring problems over several years prior to the accident or information about the controversial decision the night before the tragedy.[32]

Marshall Space Flight Center was also involved with another major NASA embarrassment, the flawed optics of the Hubble Space Telescope, which was discovered shortly after the telescope's launch on 27 April 1990. The resulting investigation could not determine with absolute certainty the cause of the spherical aberration problem, but it hypothesized how a flawed measurement of the lens's position for grinding led to a 1.3-millimeter error and to the mirror's ultimately being ground too flat at and near its edges. More troubling than the error itself was the fact that optical tests that would have found the problem had been deleted due to a variety of budget issues in the 1980s. As with the Shuttle, NASA had sold the Hubble Space Telescope to Congress and the Gerald Ford administration on the basis of a cost estimate that was far too optimistic for the level of technical complexity the project entailed. NASA

---

31. Vaughan, *Challenger Launch Decision*, chap. 9; Larry B. Rainey, Kevin B. Kreitman, Bradley A. Warner, and Stephen B. Johnson, "Critical Thinking," in *Methods for Conducting Military Operational Analysis*, ed. Andrew B. Loerch and Larry B. Rainey (Military Operations Research Society, 2007), chap. 18, pp. 607–611; Stephen B. Johnson, "Revisiting the *Challenger*," *Quest: History of Spaceflight Quarterly* 7, no. 2 (1999): 18–25.
32. Alexander Brown, "Accidents, Engineering, and History at NASA," pp. 383–388; Leveson, "Technical and Managerial Factors," pp. 251–254.

judged the technical risks of not performing these tests (which were typical on the reconnaissance satellites on which the Hubble Space Telescope optics design was based) to be acceptable.[33]

NASA's deep space projects were not spared the string of disasters. On 21 August 1993, JPL lost communications with its Mars Observer probe as it neared the Red Planet. While the cause of the accident could not be definitively determined, the resulting investigation concluded that the most likely cause was a propellant system rupture that occurred during a monomethyl hydrazine propellant tank repressurization in preparation for the Mars orbit insertion burn. The investigation board speculated that a valve leak allowed nitrogen tetroxide to leak into the propellant system tubing, such that when the repressurization occurred, the monomethyl hydrazine reacted with the nitrogen tetroxide to rupture the tubing, causing the spacecraft to spin up, which then triggered spacecraft fault protection software to stop the command sequence prior to turning on the radio transmitter back to Earth. Despite cost overruns and schedule slips that increased the cost of Mars Observer from $250 to $800 million, NASA could not ensure a successful mission. Contributing to the fiasco was the growth of the spacecraft's complexity because it was the first mission returning to Mars since the mid-1970s Viking missions; it also used a fixed-price contract. These two factors complicated the system and focused the project's attention on cost to the detriment of reliability.[34]

NASA drew three separate and inconsistent lessons from these failures. *Challenger* drew attention to technical and communication problems with regard to safety in the human flight program, and the human flight program took immediate action to fix the technical problems, oust managers that had been directly implicated in the flawed decisions, and improve safety by creating an independent safety organization at NASA Headquarters. The Hubble Space Telescope embarrassment placed emphasis on the need to ensure proper testing for large-scale robotic projects, but in the long term, the Shuttle missions to fix the optics and later to replace and improve its instruments made the Hubble Space Telescope and the Shuttle a heroic and successful combination in the eyes of the public. The embarrassments of 1990 were largely forgotten.

---

33. Robert W. Smith, *The Space Telescope: A Study of NASA, Science, Technology, and Politics* (Cambridge, U.K.: Cambridge University Press, 1993), pp. 399–425.
34. Howard E. McCurdy, *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program* (Baltimore, MD: Johns Hopkins University Press, 2001), pp. 18–19; "Mars Observer Investigation Report Released," NASA Press Release 94-01-05, 5 January 1994; Mars Observer Mission Failure Investigation Board, *MARS OBSERVER Mission Failure Investigation Board Report*, 31 December 1993.

The loss of Mars Observer contributed to an entirely different dynamic, as pressures on NASA's budget led to a new initiative to make robotic science satellites much smaller and cheaper, so that the loss of any one of them would not be a major problem.

Alternatives to Systems Management

In the 1980s and 1990s, systems management, as it had been practiced from the mid-1960s, came under increasing criticism. To many, NASA's increasingly bureaucratic system appeared unproductive and wasteful. By the early 1990s, systems management had apparently been unable to prevent major disasters and tragedies, despite its perceived high costs and bureaucratic cross-checks. External events were drawing attention to the relative failings of American management in general and to potential new approaches. NASA management, in part because of federal government directives, began to consider alternatives to improve productivity, lower costs, and provide better service to its customers.

By the early 1980s, American competitiveness in certain key industries, most prominently automobiles and commercial electronics, was declining rapidly in the face of foreign, and in particular Japanese, competitors. American management experts began to look to Japan and other nations to search for the secrets of these dramatic and unexpected foreign successes. Japanese culture, with its emphasis on cooperation instead of competition, seemed to uniquely adopt and adapt American statistical quality control methods from World War II; the Japanese created a new and powerful tool: Total Quality Management (TQM). These methods were publicized by journalists, corporate executives, and management experts and became national topics of conversation by 1981.[35]

Experimentation with TQM methods soon began in American corporations and in certain branches of the U.S. government including NASA, which became one of the early adopters of the new management technique. By 1990, TQM activities at NASA were being coordinated by the Safety Mission Quality Office at Headquarters. A report in that year boasted of a number of ongoing TQM initiatives. In 1989, Lewis Research Center won the U.S. government's Quality Improvement Award and was teaching TQM seminars to other government

35. William M. Tsutsui, *Manufacturing Ideology: Scientific Management in Twentieth-Century Japan* (Princeton, NJ: Princeton University Press, 1998); Christopher Byron, "How Japan Does It," *Time* (30 March 1981): 54–60; William Ouchi, *Theory Z: How American Business Can Meet the Japanese Challenge* (Reading, MA: Addison-Wesley, 1981); Ezra F. Vogel, *Japan as Number One: Lessons for America* (Cambridge, MA: Harvard University Press, 1979).

organizations; MSFC executives met with TQM founder Edward Deming; and SSC established a steering committee to implement a TQM program at every Center. This same report also categorized dozens of traditional activities to improve technologies and processes as TQM-related improvements, though it appears unlikely that TQM inspired or controlled many of them. Dan Goldin, who became NASA's Administrator in 1992, was a strong believer in TQM and made it an Agency priority.[36]

While many NASA organizations took TQM seriously and a number of NASA managers gave it executive-level support, NASA's rank and file remained largely skeptical. Total Quality Management's emphasis on work processes and on serving its customers seemed only marginally applicable to NASA. Many of NASA's jobs were one-of-a-kind research tasks, or development tasks that changed over the course of a project, though similar to tasks on other projects. Defining NASA's customer was even more problematic. Was the customer Congress, the President, the American people, or merely other NASA engineers that used NASA test results or analyses? Finally, how did one define the productivity and quality of NASA's products? While quality could be related to NASA's traditional quality assurance functions, productivity was not something easily quantified in NASA's nonprofit, high-creativity environment. In the end, TQM did not take hold; and by the mid- to late 1990s, TQM faded from the NASA scene.[37]

The Jet Propulsion Laboratory was relatively late in using TQM methods, beginning its TQM initiatives in 1991 under its new Director, Ed Stone, to help change JPL's culture to cut through its increasingly cumbersome bureaucracy. By 1993, Stone and his aide, Richard Laeser, recognizing that their initiative was

---

36. NASA Safety and Mission Quality Office, NASA Quality and Productivity Improvement Program, *NASA Total Quality Management 1989 Accomplishments Report*, June 1990, pp. 6–8; Peter J. Westwick, "Reengineering Engineers: Management Philosophies at the Jet Propulsion Laboratory in the 1990s," *Technology and Culture* 48, no. 1 (2007): 74.
37. Historical research on the TQM management fad at NASA has, with a few exceptions, yet to be written. For its impact on JPL, see Peter J. Westwick, "Reengineering Engineers: Management Philosophies at the Jet Propulsion Laboratory in the 1990s," *Technology and Culture* 48, no. 1 (2007): 67–91. A number of the observations made here are from the author's experience. From 1990 to 1991, the author learned TQM at Martin Marietta Corporation Astronautics, which at that time was implementing the TQM Quality Function Deployment technique of generating and assessing requirements on research programs. The author then taught these same methods to some technology R&D groups at MSFC. The problems encountered there were typical of many other attempts to deploy TQM, as the author learned from many student papers on the application of TQM to NASA, the Air Force, and industry while teaching courses on space systems management in the University of North Dakota's Space Studies Department. These observations need to be further fleshed out by research on this subject, but I have no doubt about their general validity when properly qualified by local experiences.

encountering continued resistance among JPL's regular engineering workforce, decided that the key to furthering cultural change was to focus on the lab's processes. Laeser and Stone promoted Mike Hammer's "reengineering" method, which aimed to redefine an organization's processes, starting by charting out the organization's current processes and then redesigning them to eliminate inefficiencies. Stone assigned high priority to the process teams, moving key managers to head them.[38]

The reengineering initiative did not go smoothly. It made certain processes more efficient, such as Voyager mission operations and business processes defined by the International Standards Organization. However, it also proliferated the number of processes, distributed responsibilities in an alarming manner, and intensified rank-and-file resistance to management initiatives, as process ownership increased responsibilities.[39]

The Jet Propulsion Laboratory's efforts at reengineering occurred in parallel with its efforts to respond to Dan Goldin's "faster, better, cheaper" initiatives. Prior to becoming NASA Administrator in March 1992 during the George H. W. Bush administration, Goldin had been an executive at TRW Corporation and was a strong proponent of small satellite technology, including the Space Defense Initiative (SDI) project, Brilliant Pebbles. Upon becoming the head of NASA, his encounters with the current and projected NASA budgets and massive cost overruns on the Space Station program, and the likelihood of limited future funding from Congress, led him to the realization that NASA would do little science unless these missions could significantly reduce costs. In a May 1992 speech at JPL, Goldin discussed the need to reduce spacecraft and mission costs. He elaborated on this theme over the next few months, arguing that NASA needed to build more, but smaller and less expensive, spacecraft, while taking more risks, since the loss of a smaller craft would not be a major disaster to the science program.[40]

Goldin was building on an idea that had been growing in the military and at NASA, that smaller, cheaper spacecraft were appropriate for many robotic missions. The SDI program was studying the launch of hundreds of small spacecraft to intercept and destroy ICBMs. To support this effort, it was miniaturizing a number of technologies to make small, intelligent spacecraft feasible. The $80 million Clementine project was a key demonstrator of the

38. Westwick, "Reengineering Engineers," pp. 73–83.
39. Ibid., pp. 80–84.
40. McCurdy, *Faster, Better, Cheaper*, pp. 48–55.

small satellite philosophy; it started in early 1992 to test ballistic missile defense sensor technologies by performing observations of the Moon from lunar orbit. Built and operated by NRL, its mission to gather data about the lunar surface succeeded in 1994 and provided a concrete example of the "faster, better, cheaper" concept in action. NASA's Earth science community recognized the potential of small spacecraft as well. The Small Explorer program, started in 1988, successfully launched its first spacecraft, the Solar, Anomalous, and Magnetospheric Particle Explorer, in July 1992.[41]

Another inspiration for potential reformers was Lockheed's Skunk Works. This division of Lockheed, based in Burbank, California, had created a host of revolutionary aircraft, including the World War II P-38 Lightning fighter, the P-80 and F-104 jet fighters, the U-2 and SR-71 spy planes, and the F-117 stealth fighter. However, its later fame was based on more than its innovative flying machines; its fame was based on its methods for developing them. Run by Kelly Johnson from World War II until January 1975, and after that by Ben Rich, the Skunk Works had evolved a method of using small teams for its highly secret, high-technology aircraft. Johnson developed a set of 14 rules that defined the constraints and rules to run his Skunk Works projects. These included minimal reporting but critical documentation of "important work," minimizing access by outsiders to the project, delegating authority but retaining a strong project manager, steady funding, and daily interaction with the customer to build trust. Seemingly the opposite of systems management, "faster, better, cheaper" advocates pointed to the Skunk Works approach as a legitimate alternative to systems management.[42]

Ironically, the abortive and potentially massive SEI was also a spur to the development of the "faster, better, cheaper" concept. When the George H. W. Bush administration announced SEI in July 1989, NASA responded with a 90-day study to achieve a human mission to Mars. Its massive costs convinced NSC, which Bush had created in April 1989, that NASA was far too conservative. Many Council members perceived ex-astronaut and NASA Administrator Richard Truly as a member of NASA's old guard that needed to be replaced. In early 1992, they succeeded in their goal and replaced him with Dan Goldin, who they learned was supportive of smaller innovative projects, as NASA's

41. Ibid., pp. 46–47, 53–55; Stephanie A. Roy, "The Origin of the Smaller, Faster, Cheaper Approach in NASA's Solar System Exploration Program," *Space Policy* 14 (August 1998): 153–171.
42. Ben R. Rich and Leo Janos, *Skunk Works* (Boston, MA: Back Bay Books, 1994); McCurdy, *Faster, Better, Cheaper*, pp. 90–93.

Administrator. At the same time, the Senate Appropriations Committee directed NASA to develop a plan to "stimulate and develop small planetary or other space science projects." This became the Discovery program, started later that year. By 1993, the Discovery program had two projects in place: Near Earth Asteroid Rendezvous (NEAR) and Mars Pathfinder.[43]

Goldin continued to support and push the "faster, better, cheaper" cause. In 1994, NASA established the New Millennium program to use small spacecraft to flight-test new technologies to enable science missions. Its first mission was Deep Space 1, launched in 1998, which tested ion engines and autonomous navigation technologies. The Small Satellite Technology Initiative also started in the mid-1990s, with the Lewis and the Clark Earth observation satellites. Lewis launched in August 1997, while Clark was canceled due to cost overruns the next year. Finally, the Mars Surveyor program, which consisted of three Mars probes, also used the "faster, better, cheaper" philosophy. Its first launched satellite was the Mars Global Surveyor, which reached Mars in September 1997. All in all, through the 1990s, NASA launched 16 projects related to the "faster, better, cheaper" philosophy in five major programs (Small Explorer, Discovery, New Millennium, Small Satellite Technology, and Mars Surveyor). In addition, other projects, including the proposed Pluto flyby probe, drew Goldin's attention. Under Goldin's watchful eye and direction, it underwent years of studies aimed at reducing costs even further, before it was finally approved as the New Horizons spacecraft and launched in 2006.[44]

Up through 1998, the "faster, better, cheaper" programs had an excellent rate of success, given their lower costs and the higher risks that they assumed. Of the 16 "faster, better, cheaper" projects identified by Howard McCurdy in his book *Faster, Better, Cheaper*, by the end of 1998, 11 had launched, and of these it appeared that only 2 of them had failed: NEAR failed because its orbit insertion burn around asteroid Eros failed in December 1998, and Lewis also failed. Clark was canceled before it ever flew, and thus it failed as a project as well. NEAR's mission ultimately succeeded as it successfully orbited Eros in 2000. Four more "faster, better, cheaper" spacecraft, Mars Polar Lander, Deep Space 2, Stardust, and Wide-Field Infrared Explorer were slated for launches in 1999. Goldin's initiative and prodding to implement "faster, better, cheaper" looked like a stunning success, in particular the very popular Mars Pathfinder

43. Thor Hogan, *Mars Wars: The Rise and Fall of the Space Exploration Initiative* (Washington, DC: NASA SP-2007-4410, 2007); McCurdy, *Faster, Better, Cheaper*, pp. 44–47, 55–56.
44. McCurdy, *Faster, Better, Cheaper*, pp. 6–7, 56–58.

project with its little rover, Sojourner. Unfortunately, the events of 1999 would change that impression dramatically for the worse.[45]

In the meantime, in the human flight program, NASA responded to the *Challenger* accident with several changes. The first was fixing the flawed O-ring design, followed by a variety of other improvements in the safety and reliability of the Shuttle's components and systems. The Rogers Commission also had criticized the communication between NASA's engineers and managers and between NASA organizations. To help remedy this, the management of the Shuttle Program was shifted from JSC to NASA Headquarters. Finally, the Rogers Commission indicted NASA's "silent safety program." NASA's primary response was to create an independent safety organization at NASA Headquarters. However, this seemingly appropriate move was rendered less effective because it never acquired the authority needed to fully discharge its duties. The reporting requirements from the NASA Field Centers remained unclear, and the lines of safety authority and the responsibilities of the safety groups were confused. In addition, within NASA's system, each project purchased safety support, which gave them some latitude and control over the safety function and compromised safety independence in the process.[46]

By the early 1990s, cost-cutting pressures began to affect the Shuttle Program. In the decade from fiscal years 1993 to 2002, NASA's budget declined in real terms by 13 percent. In a period in which space station (soon, the ISS) expenses were taking a larger share of NASA's budget, the budget squeeze hit not only the science programs (where "faster, better, cheaper" was being implemented in large measure due to the funding problems), but the Shuttle Program as well. From 1991, NASA reduced Shuttle operating costs 21 percent by reducing the contractor workforce from 28,394 to 22,387 and the civil service personnel from 4,031 to 2,959. By 1997, contractors and civil servants were down to 17,281 and 2,195 respectively.[47]

These cost reductions were accompanied by organizational changes that some observers believed compromised safety. To reduce costs, Administrator Goldin wanted to take NASA out of repetitive operations such as Shuttle operations, and in 1994, he directed NASA to investigate how to do so. The 1995 Kraft Report claimed that the Shuttle had become a "mature and reli-

45. Ibid., pp. 6–7.
46. Leveson, "Technical and Managerial Factors," pp. 251–252; Columbia Accident Investigation Board, *Report*, vol. 1 (Washington, DC: NASA, August 2003), pp. 99–101.
47. Ibid., pp. 102–107.

able system," that it should "consolidate operations under a single business entity" and should "restructure and reduce the overall Safety, Reliability, and Quality Assurance elements" without compromising safety. These recommendations were accepted and led to the creation of the Space Flight Operations Contract, in which Lockheed Martin and Rockwell created a joint venture called United Space Alliance, to which NASA awarded a sole-source contract for Shuttle operations in 1995. The new managerial arrangement led to a new relationship between NASA and Shuttle safety, known as "insight" instead of "oversight." This meant that instead of directly monitoring and managing the work of NASA and contractor safety personnel, United Space Alliance ran the safety program and provided management with certain contractually agreed information. In 1998, Congress directed NASA to plan for eventual privatization of the entire Shuttle Program. Among other things, this would have made astronauts private employees. Another managerial move was to shift Shuttle Program management from NASA Headquarters back to JSC, which returned the Program to the pre-*Challenger* organizational structure, reversing changes made in response to the Rogers Commission recommendations. Some considered this a safety issue, as the move to Headquarters had been made to improve program communications.[48]

Both in robotic and human flight programs, NASA's emphasis in the 1990s had shifted away from concerns for safety and reliability to pressures to reduce costs. Despite the inherent riskiness of spaceflight, complacency had set in, and it was only a matter of time before it would be shattered.

The End of "Faster, Better, Cheaper," *Columbia*, and the Columbia Accident Investigation Board

For NASA's robotic spacecraft programs, and in particular its Mars science program, 1999 marked the end of an era . . . the "faster, better, cheaper" era. In March, the Wide-Field Infrared Explorer failed shortly after launch when the frozen hydrogen used to cryogenically cool its detectors vented into space after the spacecraft's protective cover was prematurely ejected. It was the fifth spacecraft in the Small Explorer program. In the meantime, three Mars spacecraft were on their way to the Red Planet: Mars Climate Orbiter, Mars Polar Lander, and Deep Space 2. Mars Climate Orbiter was intended to perform observations of the Martian atmosphere from orbit. Mars Polar Lander and Deep Space 2

48. Ibid., pp. 107–110; Leveson, "Technical and Managerial Factors," pp. 256–257.

had been launched together, aiming to land near the poles, with Deep Space 2 containing two subsurface probes to search for water ice.

Hopes were high as Mars Climate Orbiter approached Mars in September 1999. In the week prior to Mars orbit insertion, mission navigators noticed that the spacecraft's trajectory seemed closer to Mars than expected. As it made its closest approach, mission controllers awaited the signal from the spacecraft indicating it had achieved orbit. That signal never came, and attention quickly focused on the odd trajectory. The trajectory problem turned out to hinge on a unit conversion problem. The files delivered from contractor Lockheed Martin had their propulsion maneuvers defined in English units, instead of the specified metric units. The difference was 4.45, the conversion factor of newtons to pounds. The difference in units led to an error conversion factor of 4.45 in the estimated effect of trajectory corrections, and as a result the spacecraft went too close to Mars and burned up in the atmosphere. The operations teams that might have otherwise noticed the error were smaller than on many previous missions, due to the reduced budgets of "faster, better, cheaper."[49]

In December, more bad news, or more accurately, no news at all, came from Mars. Both Mars Polar Lander and Deep Space 2's two probes seemed to be working properly as they entered their entry, descent, and landing phases. None were heard from again. Deep Space 2's failures were never definitively determined, but possibilities ranged from soil being significantly harder than planned when the probes hit the surface, to handling problems at KSC prior to launch that inadvertently sent an electrical pulse that mimicked separation and turned on their batteries, draining them of power.[50]

The investigation of the Mars Polar Lander failure provided a more definitive cause. To detect touchdown, the spacecraft used Hall Effect sensors that detected movement of the spacecraft legs. Leg deployment produced transient signals in these sensors. During deployment, it is almost certain that these transient signals were processed by the software as the real touchdown, turning off the engines while the spacecraft was well above the surface; the spacecraft crashed to the surface and was destroyed. During development, the transient signal problem was known, but the software requirement had been written in such a way that, when ultimately coded, it did not properly meet the intent of

49. McCurdy, *Faster, Better, Cheaper*, pp. 6–7; David M. Harland and Ralph D. Lorenz, *Space Systems Failures: Disasters and Rescues of Satellites, Rockets, and Space Probes* (Chichester, U.K.: Springer-Praxis, 2005), pp. 339–341.
50. Harland and Lorenz, *Space Systems Failures*, p. 239.

the requirement. Testing of the descent and landing did not catch the problem because one of the landing legs was wired incorrectly during this test. After the wiring had been fixed, the test was not rerun due to tight schedules and budgets of the "faster, better, cheaper"-style project.[51]

The failure of all three Mars missions in 1999 drew unwanted attention from both NASA executive management and the press. Mars missions always drew significant interest, and the failure of all three provided strong evidence of programmatic problems. The various failure investigations implicated reductions in testing and in systematic safeguards and cross-checks. In other words, "faster, better, cheaper" had cut more than the fat and into the meat of systems management, leading to failures. Management at JPL reassessed its project management and systems engineering methods, and it found them wanting. Culture change and reengineering distracted management from its core activities and diluted responsibilities. In 2001, Charles Elachi took over for Ed Stone as Director of JPL, and he quickly reinvigorated JPL's historical systems engineering methods and traditions. The lab increased funding for individual projects and reinstituted rigorous design reviews. "Faster, better, cheaper" was out, and systems management was back.[52]

Two years later, on 1 February 2003, a crowd of guests was waiting at KSC for the Space Shuttle *Columbia* to return from its mission to perform a variety of microgravity experiments in low-Earth orbit. Like JPL's mission controllers in 1999, they waited in vain. *Columbia* had broken up over east Texas and was destroyed, along with its crew of seven. The resulting investigation concluded that hot plasma had entered a hole in the leading edge of the Shuttle's left wing, which burned through the structure. The wing fell away, and the Shuttle lost control, tumbled, and broke apart. The hole in the leading edge was created during ascent 17 days before, when insulation foam from the external tank fell off and hit the leading edge at high speed.[53]

Further investigation into the causes of the accident uncovered a trail of events both prior to the fated flight and during the flight itself. Much like the problems leading to the *Challenger* accident 17 years before, foam debris falling off the external tank during ascent was a problem that had been going on from the inception of the Shuttle Program. Also like *Challenger*, this behavior had been reclassified over time from a major safety concern to a minor maintenance

51. Ibid., pp. 330–331.
52. Westwick, "Reengineering Engineers," pp. 84–87.
53. Columbia Accident Investigation Board, *Report*, vol. 1, chaps. 2 and 3.

issue. Foam strikes during ascent had caused minor damage to the Shuttle's thermal protection system on many flights, leading to repairs between flights. Some of the foam pieces, particularly those from the "bipod ramp," were quite large and caused significantly more damage. The real risks of external tank debris hitting the orbiter were misunderstood and underestimated, while the costs to fix the problem were considered too high.[54]

Decision-making during *Columbia*'s flight was also flawed, very much like the decision-making the night prior to *Challenger*'s final flight. During ascent, cameras photographed the foam strike hitting the left wing's leading edge. Shuttle engineers began to assess the potential damage, and even reporters began asking questions about it. Ultimately, the engineers could not determine the actual damage but were worried enough to inquire into the possibility of using a military reconnaissance satellite to photograph the suspect area. Because this request did not go through proper channels, NASA management stopped it. Poor organizational structure inhibited engineering information from making its way to management. Management believed that, even if there was a problem, nothing could be done about it in flight, so it did not make much sense to make extraordinary efforts to determine the amount of damage. Changes in personnel made estimates of the foam strike damage problematic, because the model used to do the estimate was not valid for large pieces such as the one that hit *Columbia*, and the new personnel were unaware of this limitation.[55]

The Columbia Accident Investigation Board noted the many similarities between the organizational and communication problems leading to the *Challenger* and *Columbia* accidents. While finding several managers at fault, the Columbia Accident Investigation Board ultimately found the causes of the accident to be much more insidious than the Rogers Commission had. Some of the major organizational issues the Columbia Accident Investigation Board emphasized included the following:

- Conflicting goals of cost, schedule, and safety, in which safety lost out.
- Overemphasis on bureaucratic procedures, to the detriment of engineering insight and expertise.
- An organization and structure that blocked effective communication of technical problems.

54. Ibid., pp. 121–131.
55. Ibid., pp. 140–172.

- Changes to the safety organization that eroded NASA's safety expertise by transferring safety tasks and responsibilities to contractors.
- A lack of resources, independence, authority, and personnel in NASA's safety organization to supply alternate perspectives to developing problems.

Whereas the Rogers Commission cited violations of NASA's procedures, the Columbia Accident Investigation Board concluded that since these issues were common to both the *Challenger* and *Columbia* accidents, the problems leading to the accidents were inherent to NASA itself, part of its "organizational culture." NASA's traditional methods of fixing the technical problems and tightening its procedures was not going to work, since the technical problems were caused by violations of those very organizations, processes, and procedures.[56]

After *Columbia*, NASA quickly went to work to fix the difficult problems with the external tank foam insulation and scrubbed various problematic aspects of the Shuttle's design and operations. It took a number of organizational measures following the Columbia Accident Investigation Board recommendations. It shifted control of the Shuttle Program from JSC back to NASA Headquarters (following the precedents of Apollo and the post-*Challenger* organization). It established the Safety, Reliability and Quality Assurance organization at Headquarters. Flight Readiness Review procedures were modified to allow engineers to participate, and they required astronaut managers to participate and sign off on the launch decision. The Agency established the NASA Engineering and Safety Center at LaRC (and later a second NASA Safety Center at Glenn Research Center), which was tasked to independently review recurring anomalies and act as a resource for connecting engineering to safety issues. Another Columbia Accident Investigation Board recommendation was the creation of an Independent Technical Authority (ITA), which NASA began to implement in November 2004. The ITA funded "Technical Warrant Holders" as technical experts to assess engineering and safety designs and decisions. Ultimately, the ITA was transformed, in February 2006, into a process known as "Process-Based Mission Assurance" (PBMA), which emphasized the development of "technical excellence" as the basis of building safety into NASA's systems. As it evolved, the ITA/PBMA was intended to provide a separate line of communication for technical personnel to air problems. This reinvigorated a matrix manage-

56. Ibid., chaps. 7 and 8, esp. pp. 199–202.

ment system in which personnel reported both to project managers (who controlled the funding and schedules for projects) and functional managers (who controlled the technical content and personnel). Under the new system, the functional managers were tasked with ensuring technical quality and acting as counterbalances to the project managers. The Columbia Accident Investigation Board was far less specific in its recommendations on how NASA should change its culture, and NASA itself had great difficulty trying to determine how to interpret that mandate.[57]

NASA concluded that it needed help with culture change, and in December 2003 it sent out an RFP to perform cultural analysis to pinpoint cultural problems that affected safety and then take measures to fix them. Over 40 bidders responded, and in March, NASA hired Behavioral Science Technology (BST), who then instituted cultural surveys across the Agency; and in a February 2005 report, BST stated that significant progress was being made in cultural change, as measured by its surveys. One new initiative was to train managers to be more open to engineering opinions.[58]

Major changes in NASA personnel and programs quickly began to shift attention away from the Columbia Accident Investigation Board recommendations. *Columbia*'s demise made it clear that the replacement of NASA's Shuttle fleet could no longer be postponed, and this led to a broader assessment of what NASA's goals should be. The result of these discussions was the speech by President George W. Bush in January 2004, announcing the Vision for Space Exploration to complete the Space Station by 2010, retire the Shuttle, conduct the first human mission with a new Crew Exploration Vehicle by 2014, and return to the Moon by 2020. The next month, NASA

---

57. Diane Vaughan, "System Effects: On Slippery Slopes, Negative Patterns, and Learning from Mistake," in *Organization at the Limit: NASA and the Columbia Disaster*, ed. William Starbuck and Moshe Farjoun (Oxford, U.K.: Blackwell, 2005); author's conversation with Michael Griffin, 26 April 2007; "NASA Announces New Safety Center," NASA Press Release, 11 October 2006, available at *http://www.spaceref.com/news/viewpr.html?pid=21031* (accessed 31 January 2009); "Final Report of the Return to Flight Task Group," July 2005, pp. 95–110, available at *http://www.scribd.com/doc/995714/NASA-125343main-RTFTF-final-081705* (accessed 31 January 2009); "Technical Excellence/Technical Authority," 16 March 2006, available at *http://pbma.nasa.gov/index.php?fuseaction=ita.main&cid=501* (accessed 31 January 2009).
58. "NASA Enlists Behavioral Science Technology, Inc. to lead agency-wide culture change," *EDP Weekly's IT Monitor* (26 April 2004), available at *http://findarticles.com/p/articles/mi_m0GZQ/is_17_45/ai_n6264746*; *http://www.FindArticles.com* (accessed 31 January 2009); John Schwartz, "Some at NASA Say Its Culture is Changing, but Others Say Problems Still Run Deep," *New York Times* (4 April 2005), available at *http://query.nytimes.com/gst/fullpage.html?res=9D03EEDB1E3FF937A35757C0A9639C8B63&sec=&spon=&pagewanted=all* (accessed 31 January 2009).

released its initial interpretation of the Vision. A presidential commission gave its assessment in June.[59] NASA established the Exploration Systems Mission Directorate to implement the exciting new program, and NASA's attention quickly shifted to its implementation. Michael Griffin took over from Sean O'Keefe in April 2005. Griffin, who was without question the most technically educated Administrator NASA had had to date, had his own strong opinions about how to address NASA's problems, and BST's cultural surveys were not among them. In June 2005, he terminated the BST contract. He believed that one of the most important things that NASA needed was an organizational structure that provided alternate communication lines for engineering and safety concerns, which was provided by the ITA/PBMA organizational structure and processes. By early 2009, the culture issue, while not forgotten, did not have the priority it had had in the immediate aftermath of the *Columbia* tragedy.[60]

The Social Nature of Failure

Even though much of NASA's attention had shifted from the difficult and uncertain problems of its culture to a new and exciting program of exploration, the culture problem had not gone away. Dealing with the issue remained problematic due to the inherent slipperiness of the concept. The Columbia Accident Investigation Board *Report* described "organizational culture" as "the basic values, norms, beliefs, and practices that characterize the functioning of a particular institution." Explaining further, "organizational culture defines the assumptions that employees make as they carry out their work; it defines 'the way we do things here.'"[61] Something in these basic values, norms, beliefs, and practices led to catastrophic system failure. NASA's problem was, and is, to determine the connection between culture

---

59. President Bush Announces New Vision for Space Exploration Program, "Remarks by the President on U.S. Space Policy," Press Release, 14 January 2004, available at *http://history.nasa.gov/Bush%20SEP.htm* (accessed 31 January 2009); NASA, *The Vision for Space Exploration* (Washington, DC: NASA, February 2004); *A Journey to Inspire, Innovate, and Discover: Report of the President's Commission on Implementation of United States Exploration Policy* (Washington, DC: GPO, June 2004); Frank Sietzen, Jr., and K. L. Cowing, *New Moon Rising: The Making of America's New Space Vision and the Remaking of NASA* (New York, NY: Apogee, 2004); "NASA pulls plug on culture change contract," *Industrial Safety & Hygiene News* (1 August 2005), available at *http://www.highbeam.com/doc/1G1-135467272.html* (accessed 31 January 2009).
60. "Michael Griffin Takes the Helm as NASA Administrator," NASA Press Release, 14 April 2005, available at *http://www.nasa.gov/about/highlights/griffin_admin.html* (accessed 31 January 2009); author conversation with Griffin, 27 April 2007.
61. Columbia Accident Investigation Board, *Report*, vol. 1, p. 101.

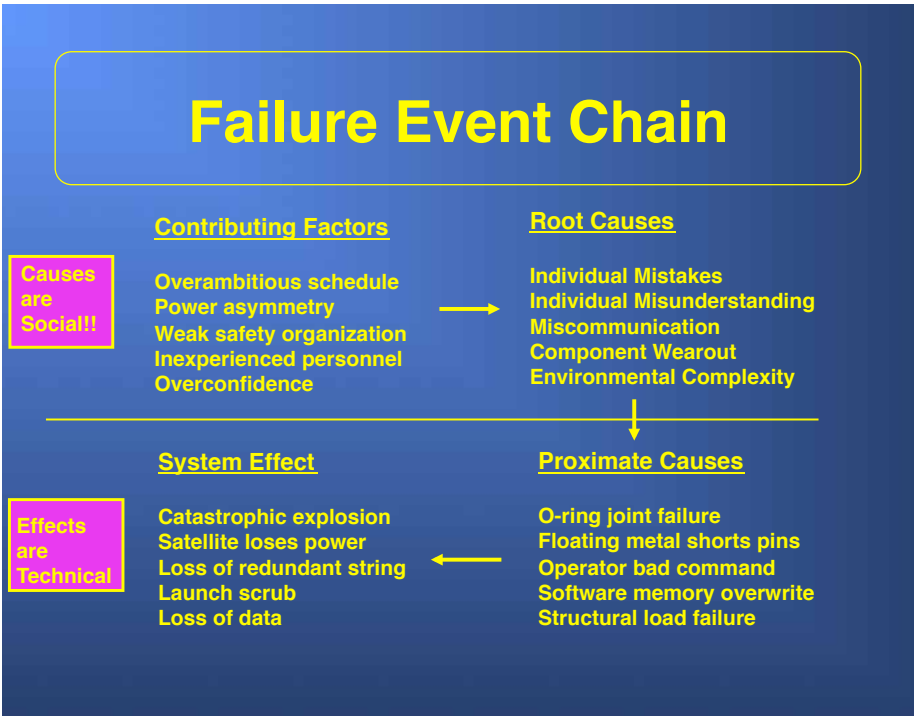

Figure 1: Failure chain of events. *Courtesy of Stephen B. Johnson*

and failure and then to make improvements to culture so as to reduce failure rates and criticality.

To make this connection, we need to understand the nature of failures. In engineering terms, failure is defined as "the unacceptable performance of intended function or the performance of an unintended function."[62] That is, when the system can no longer do what it was designed for, or does things that it was not intended to do, it has failed. Failure is generally the outcome of a chain of events, which are made more likely by various contributing factors. Failure investigations start by assessing the final failure effects, which can include complete system loss, like the Space Shuttle *Columbia*'s burning up in the atmosphere, or can be more benign, such as the scrub of a Shuttle

62. This definition, which is in development on the Constellation program, draws from a variety of engineering sources and has a few improvements to those earlier definitions. See Stephen B. Johnson, "Introduction to System Health Engineering and Management in Aerospace," *Proceedings of the First International Forum on Integrated System Health Engineering and Management* (Napa, CA, November 2005).

launch. The proximate causes of these failures are generally the technical items that malfunctioned and led to the failure effects, such as the O-ring failure of the *Challenger* accident or the foam that fell off the external tank and hit *Columbia*'s wing during ascent. But proximate causes have their genesis in root causes, such as human-induced errors in the application of the foam to the external tank in the *Columbia* case, the decision to launch *Challenger* on a morning when the temperature was lower than rated environmental limits, or human error in creating the Shuttle's original flawed SRB segment joint design. Finally, there are contributing factors, such as pressures to launch the Shuttle on an accelerated schedule, pressures to lower costs, or use of a teleconference instead of a face-to-face meeting contributing to miscommunication.

Frequently the failure effects and the proximate causes are technical, but the root causes and contributing factors are social or psychological. Successes and failures clearly have technical causes, but a system's dependability strongly depends on the human processes used to develop it, the decisions of the funders, managers, and engineers who collectively determine the level of risk. Fallible humans make individual cognitive or physical mistakes, or they make social errors through lack of communication or miscommunication.

Although the statistics have not been studied fully, my sense from experience in the field and from discussions with experienced engineers is that 80 to 95 percent of failures are ultimately caused by individual human errors or social miscommunication between individuals and groups. Most of these are quite simple, which makes them appear all the more ridiculous after the fact when the investigation gets to the root cause and finds, for example, the Mars Climate Orbiter's English-to-metric-unit conversion problem, a nut or bolt left inside the propulsion system (a Centaur failure in 1991), a reversed sign or wiring (for example, the Total Ozone Mapping Spectrometer—Earth Probe), or a single digit left off a command sequence (Phobos 1). Contrary to popular belief, it is the very banality of the causes that makes them so hard to find. We constantly carry out simple daily tasks and communications. Thousands of such tasks and communications happen every day on a project, and any one of them can be the cause of tomorrow's dramatic failure.[63]

---

63. Harland and Lorenz, *Space Systems Failures*. This book catalogs many types of failures, though it in general discusses the proximate as opposed to root causes.

Failure, then, is caused by a fault, which is defined as "a physical or logical cause, which explains a failure."[64] Faults can be proximate causes or root causes, where the root cause is the first event in the explanatory chain of events. The vast majority of root causes, if pursued far enough, are due to individual or group mistakes by humans. This should be no surprise. Technologies are merely the final products of human knowledge applied to creating useful artifacts, and an artifact merely embodies and incarnates knowledge from its creators. Hence if an artifact has a fault, this is ultimately due to a flaw in the knowledge of its creators or in a mismatch between the knowledge of its creators and that of its users.[65]

Making a system dependable is akin to the problem of reducing the number of needles in haystacks. Most problems are very simple in their causes (the needles), and it is best to prevent them to begin with, as finding them amid all the complexities of the design and how it operates in all possible conditions (the haystack) is very difficult. In essence, dependability is gained by minimizing the number of initial mistakes (fewer needles) and testing the system to find the inevitable mistakes that occur (finding and removing the remaining needles). Skunk Works or "faster, better, cheaper" approaches can succeed because small, experienced teams make fewer mistakes because there are simply fewer people, and with experience they make fewer mistakes as individuals, and also because having fewer people reduces the number of interactions between people where miscommunication may occur. In addition, experienced personnel have the intuition to sense where the remaining mistakes are likely to be found, so they can target their relatively smaller documentation and testing to find them. However, over the long run, small teams cannot provide repeatable results. That is because humans are unable to maintain focus for long periods. Eventually we become lax and forget a

64. This definition is drawn from ongoing work on failure terminology in NASA's Constellation program. It uses many prior engineering sources (from both from academia and industry) and also draws from insights in the philosophy of science that emphasizes that much of science is really about "explanation." From this point of view, a failure is a phenomenon that requires explanation, and a fault is the explanation. B. C. van Fraasen, *The Scientific Image* (Oxford, U.K.: Oxford University Press, 1980), pp. 132–134; Ronald N. Giere, *Explaining Science: A Cognitive Approach* (Chicago, IL: University of Chicago Press, 1990), pp. 104–105. Giere hypothesizes that scientific explanation is characterized by the use of models. This accords well with many explanations of failure, by reference to specific hypothesized failure modes, often backed up by analysis, simulation, and testing.

65. The remaining 5 to 15 percent of faults are caused by a lack of knowledge about the environment in which the system operates. An example of this would be the lack of understanding of the near-Earth space environment and high radiation levels in the Van Allen Radiation belts in the early Space Age, or how the zero-g environment for satellites caused particles to float and short out electronic components.

key detail or skip a critical process because "we know" that we have done the right things and don't need to doublecheck.

By contrast, systems management and systems engineering reduce failure rates by providing formal cross-checks that catch and fix most potential mission-ending faults. Systems management and systems engineering cannot guarantee absolute success, but history shows that they do significantly reduce project failure rates.[66] This should be no surprise, because this is one of the major reasons why they were created to begin with. Systems management is needed when a project gets so large that the simple communication of small teams breaks down. This certainly is the case for huge projects such as Apollo or the Space Shuttle, but also for larger robotic systems and for teams that are distributed or have contracting or other barriers to communication.

The recognition that individual and social (cognitive, communicative, and organizational) factors are critical to system dependability has been slowly growing. The Columbia Accident Investigation Board's *Report*, with sections on organizational culture that largely drew from, and were partly written by, sociologist Diane Vaughan (who had written the authoritative book, *The Challenger Launch Decision*), was a major milestone in documenting and broadcasting this fact to NASA, but, as noted above, it fell short of providing a framework for or specific solutions to the problem. Dozens of failure investigations have concluded that individual (operator or design error) or social (communication) factors are implicated in failure. The demise of "faster, better, cheaper" and the renewed emphasis on systems management in NASA's robotic programs is also an indicator that management and engineering "philosophies" matter. However, an academic and theoretical framework has been lacking, and those that have been developed are currently little known. It is unlikely that approaches driven primarily by the social sciences are going to have much impact on NASA's engineers. What NASA engineers and managers are more likely to understand and implement are ideas couched in engineering terms that draw from social science research, instead of the other way around.

One recent approach to the problem has been developed by Nancy Leveson at MIT. Leveson, a safety engineer and researcher, developed modeling techniques that could begin to address the safety implications of the culture

66. On early missile, launcher, and satellite projects without these methods, failure rates of 50 percent were typical. After implementation of systems management, failure rates decreased to around 5 percent. Not all of this was due to systems management, as other learning and design improvements were occurring. Nonetheless, systems management deserves some of the credit. See Johnson, *Secret of Apollo*.

issue. To move forward, she looked backward, resurrecting the decades-old methods of systems dynamics developed at MIT in the late 1950s and 1960s by Jay Forrester.[67]

Forrester, who was one of the leaders of the Whirlwind and Semi-Automatic Ground Equipment (SAGE) real-time computer projects for air defense in the 1950s, became restless with this work and joined MIT's Sloan School of Management in 1956 to apply computer simulation methods to develop new management methods. His 1961 book, *Industrial Management*, showcased his simulations of corporate decision-making, which he and his students modeled as a feedback information system with time-critical information flows for making management decisions. Forrester broadened his approach in 1969, developing models of cities on a similar simulated basis, and published *Urban Dynamics*, which again showcased his interactive simulations that contained multiple interacting feedback loops that indicated to Forrester that decision-makers were unable to make proper decisions without computer-based modeling assistance. Finally, Forrester won funding from the Club of Rome, a small international group of prominent businessman, scientists, and politicians, to apply his methods on a worldwide scale. His models grouped the world into five major subsystems: natural resources, population, pollution, capital, and agriculture. The results of these models led to the controversial but widely circulated *Limits to Growth*, published in 1972, which argued that human civilization would, sometime around 2050, have a catastrophic collapse. Forrester's work was a forerunner of many comprehensive global environmental models and drew from his background in control systems and cybernetics as well as the newly developed techniques and technologies of computing.[68]

Leveson believed that NASA's culture and safety problem was ripe for a similar approach, and she began to model NASA's safety organization and decision-making. Her results, like those of Forrester's in the 1950s and 1960s, showed a periodic roller coaster behavior of concern for safety with a cycle

---

67. Leveson, "Technical and Managerial Factors," pp. 239–245; Nancy G. Leveson, *System Safety: Back to the Future*, unpublished book draft, available at *http://www.sunnyday.mit.edu/book2.html*.
68. Paul N. Edwards, "The World in a Machine: Origins and Impacts of Early Computerized Global System Models," in *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After*, ed. Agatha C. and Thomas P. Hughes (Cambridge, MA: MIT Press, 2000), pp. 221–253; Kent C. Redmond and Thomas M. Smith, *From Whirlwind to MITRE: The R&D Story of the SAGE Air Defense Computer* (Cambridge, MA: MIT Press, 2000); Jay Forrester, *Industrial Dynamics* (Cambridge, MA: MIT Press, 1961); Jay Forrester, *Urban Dynamics* (Cambridge, MA: MIT Press, 1969); Donella H. Meadows et al., *The Limits to Growth: A Report for the Club of Rome's Project on the Predicament of Mankind* (New York, NY: Universe Books, 1972).

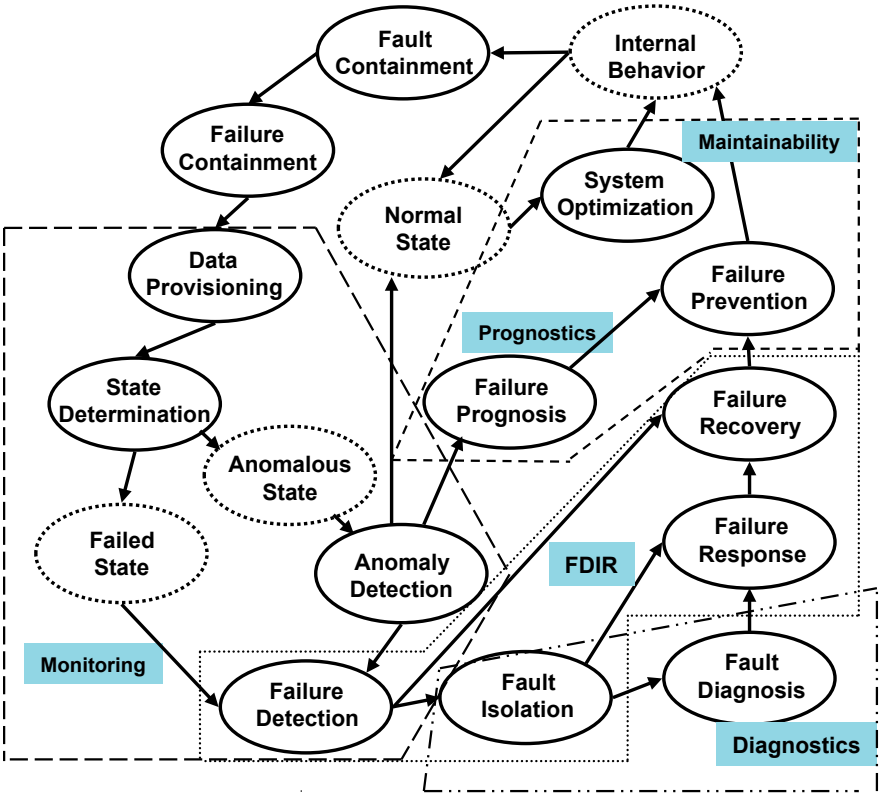

Figure 2: System health management functional flow. *Courtesy of Stephen B. Johnson*

time of roughly 15 to 20 years (NASA's actual human flight accidents showed a 17-year cycle). That is, after spikes of great safety concern immediately following major accidents, NASA quickly reverts to its regular behavior with relatively low, and decreasing, concern for safety. Leveson and her students continue to use these models to hypothesize the impact of potential changes to NASA's organizational dynamics on its safety outcomes.[69]

Another approach, developed primarily by this author with many others contributing since the late 1980s, also uses control theory insights, along with others from systems engineering and from the history, sociology, and philosophy of science and technology. In this approach, the general concern is for system dependability, which is defined as "the ability of a system to function

69. Leveson, "Technical and Managerial Factors," pp. 239–245.

in a manner meeting human expectations." Another term for this budding discipline is "system health management." In this view, as with Leveson's, complex systems such as those required for human and robotic spaceflight are complex mixtures of humans and machines, and from the standpoint of dependable systems, the functions needed to make systems dependable can be allocated to people, software, or hardware. In an operational system, the functions needed to monitor, predict, detect, isolate, respond, and recover from internal failures are arranged into control loops, and those loops are potentially analyzable in terms of time and criticality to create a system architecture that can successfully respond to impending or existing failures. The design of such a system requires new processes that are only partially understood as of yet.[70]

Creating dependable systems requires a proper mix of prevention of failure and the mitigation of internal failures. Humans are ultimately responsible for all dependability functions, but some functions can be placed in hardware or software. Even if placed in hardware or software, these functions are still designed based on human knowledge and intentionality. It is assumed that human designers, operators, and analysts are all fallible, with a certain probability of making mistakes, depending on various "contributing factors" of their social environment. These errors are just as likely to occur in design as in operations.

Certain well-known design principles, such as "clean interfaces," are reconceptualized as principles based on the minimization of communication errors between people, so that reducing the complexity of the functions between system components reduces the needed communications between individuals within differing organizations and their different "cultures." The principle of analytical independence, often seen as crucial for safety purposes, is seen as impossible to achieve in any one person, since complete independence also means no knowledge of the application and hence no ability to constructively say anything about it. Instead of trying to find that mythical single organization or person that can be independent, multiple knowledge overlaps based on differing principles and approaches are needed to achieve plausible results while cross-checking for errors.[71]

---

70. Johnson, "Introduction to Integrated System Health Engineering and Management." The first publication of this "closed-loop operational architecture" appeared in Jeffrey Albert, Dian Alyea, Larry Cooper, Stephen Johnson, and Don Uhrich, "Vehicle Health Management (VHM) Architecture Process Development," *Proceedings of SAE Aerospace Atlantic Conference* (May 1995, Dayton, OH).
71. Ibid.

A reorientation of NASA's thinking is needed, from seeing technical problems as purely technical to understanding that they are primarily flaws in individual knowledge, performance, and social communication. If pursued, these insights may lead to significant improvements in NASA's organizational culture. Diagnosing the culture problem need not be mysterious. One needs only to pursue all failure investigations back to their individual and social roots to identify the individual and organizational flaws that must be addressed. Deciding exactly how to address those problems is more problematic; but by the nature of the problem, it will involve education and training for individuals and changes to institutional structures and processes to improve organizational communication. Technical improvements can also assist, by finding ways to pinpoint which processes correlate with certain kinds of errors and then providing automated means of cross-checking for those error types.

Conclusion

System dependability and system safety, and their inverses, system failure and system hazards, are ultimately functions of individual and social understandings, communications, choices, and actions. Technical systems fail because they embed human failings, mistakes, and misunderstandings. It is unlikely that significant improvements to dependability and safety can be made until engineers and managers learn that ultimately they themselves are the causes of failure and that several individual and social actions must also be taken, along with technical improvements, to improve these qualities.

As Henry Petroski elegantly narrated in his studies of failure, there is an alternating pattern of conservatism and innovation in design over the course of engineering generations, which is rooted in the long-term trends of cultural factors. Failures result more frequently at the end of "innovation periods" as cost cutting and design originality push past reasonable limits. The fact of having pushed too far is generally revealed by the failures themselves. The resulting investigations, if pressed far enough, uncover the individual and social causes of the failures.

NASA has displayed this same dynamic. In JPL's deep space programs, just getting into space was a highly innovative effort that entailed much learning and many failures. In this brief but exciting period from the late 1950s to the early 1960s, JPL's managers, engineers, and contractors discovered many things about the space environment and about how to change its own institutional structures and organizations to operate spacecraft in that environment. A long stable period, with growing conservatism and creeping bureaucracy, ensued from the mid-1960s to the mid-1980s. The encroaching bureaucracy, limited

funding, and recognition of alternate methods both within (mainly from the Strategic Defense Initiative) and without (the TQM fad) the space industry bred a growing discontent; and by the late 1980s and early 1990s, JPL was pressed into, and also decided to adopt, new TQM, "faster, better, cheaper," and Skunk Works methods. A short period of institutional change ensued, with a number of successful lower-cost projects at JPL and elsewhere. However, the failures of 1999, with their associated bad publicity, showed the limits of "faster, better, cheaper," and the pendulum swung back to conservative design with systems engineering.

The human flight program showed a similar dynamic, but on a shorter timescale. In the early human flight programs of Mercury and Gemini, NASA successfully navigated the treacherous hazards of space, though sometimes by a hair's breadth (such as Gemini 8, in which Neil Armstrong played a critical role in averting disaster). It accomplished this despite, and perhaps because of, the fact that nearly everything it did was new. However, success bred overconfidence, which was shattered by the Apollo 204 accident of 1967. The resulting investigation uncovered many other design problems besides the one(s) that killed the crew. Many Apollo veterans acknowledged that the enforced pause after the accident probably saved the program by rooting out and fixing many other impending technical and organizational problems. The Skylab and early Shuttle programs also succeeded despite the major new technologies, probably for similar reasons to those of the Mercury and Gemini projects, as engineers paid close attention to every detail for these new systems. But once again, latent problems compounded by reduced attention to safety led to the *Challenger* disaster of 1986. A round of safety improvements, augmented by a few more organizational changes, produced solid results for the next 17 years. However, cost cutting and safety reductions took their toll by the late 1990s, and these in turn contributed to the 2003 *Columbia* tragedy.

After the Columbia Accident Investigation Board *Report*, the resulting investigation went beyond the usual culprits of engineering and management structures, flawed decisions, and technical problems to indict NASA's organizational culture as inherently flawed. While the diagnosis was true, it was vague, and NASA's managers and engineers found it mostly "non-actionable." NASA made some specific and beneficial organizational and process changes, but the broader issue of culture, for which NASA hired BST, for the most part did not get addressed because NASA could not determine exactly what it meant, and BST likely did not understand the uniqueness of NASA's culture and how to develop precise and convincing actions. The NASA culture problem remains largely unresolved.

The culture problem at NASA has not gone away, but cultural change at NASA is no longer a major priority. However, the relationship of culture to dependability and safety has not gone unnoticed, and efforts to make the connection between the two are under way. While NASA's initial efforts at cultural change were stymied by a lack of understanding of the relationship of individual and social factors to failure, significant progress has been made in understanding these relationships. This bodes well for the future of NASA's programs, but only if the Agency both learns from its past and makes use of these growing insights from its own history.